EXHIBIT I

Labaton Sucharow

Jonathan Gardner
Partner

212 907 0839 direct
212 907 0700 main
212 883 7063 fax
jgardner@labaton.com

New York Office
140 Broadway
New York, NY 10005

September 7, 2022

VIA ELECTRONIC MAIL
Randall W. Edwards
O'Melveny & Myers LLP
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111
redwards@omm.com

Re: Samsung Filing

Dear Counsel:

I write in response to your September 6, 2022 letter and accompanying Samsung employee affidavit ("Samsung's Affidavit"). Your letter and Samsung's Affidavit wholly ignore several of Claimants' claims,[1] is rife with misstatements of facts and overlooks the applicable case law. Critically, your letter and Samsung's Affidavit **admit** to converting a user's facial landmark data to numerical values and storing the data on users' devices which is a violation of BIPA.

According to Samsung's Staff Engineer, Samsung's technology automatically scans every photo to determine whether it has been analyzed for "face clustering," determines whether a face is detected in the image, analyzes each face for "landmarks" to "align" the facial image, extracts those key facial features, and converts said data into "vectors," each of which is assigned a numerical value

[1] For example, Your letter and Samsung's Affidavit continue to ignore the other features and technology Claimants identified over the last four (4) months including, but not limited to, (i) the functionality of the Gallery App and its "Camera Features" that integrate artificial intelligence "smart features;" (ii) Samsung's "Selfie camera," which employs facial processing techniques by repeatedly scanning the image frame to detect a user's face; (iii) Samsung's "Live Focus Video," which allows users to add filters and effects to videos, (iv) "Bixby Vision," which provides "helpful information based on what [the user] see[s] through the camera," (v) "AR Emoji," which allows users to create emojis of themselves and use or apply filters and stickers, (vi) "Single Take," which allows users to capture a "series of photos and short videos all at once, and then choose the best one from the Gallery," (vii) the Samsung Gallery Application "tagging" features, (viii) the Gallery Application's use of facial processing systems, algorithms, and facial recognition techniques including, but not limited to, image analysis; and (ix) Samsung's use and continued development of systems and methods that collect facial data as evidenced by patents issued by the United States Patent Office ("USPTO") to Samsung discussing the use of and/or application of facial and/or face recognition technology, techniques for scanning facial geometry, and collection and use of facial geometry and related data.

corresponding to a specific facial feature. Samsung Affidavit at ¶¶ 2, 8, and 11. Once the vectors have been assigned, the Clustering Engine analyzes the vectors to determine if the similarity values between the analyzed image and other images stored locally on the device are high enough to "cluster." *Id.* at ¶ 12. By analyzing the face for landmarks, extracting key facial features, and converting that data into vectors, which are then assigned numerical values, Samsung is generating a mathematical representation of the user's face. Simply put, the numerical values Samsung generates that correspond to users' specific facial features is biometric information. *See Id.* at ¶ ¶ 2, 6-16. *See also generally, Rivera v. Google*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017); *Vance v. Amazon*, 525 F. Supp. 3d at 1301 (W.D. Wash 2021); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1277 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021); *Sosa v. Onfido, Inc.*, No. 20-cv-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022); and *Hazlitt v. Apple Inc,* 500 F. Supp. 3d 738 (S.D. Ill. 2020).

Furthermore, even if we accept your statements as true, it is irrelevant whether the collected data actually identifies the individual. *See* Samsung's Affidavit at ¶ 13. *See Vance v. Int'l Bus. Machines Corp.*, No. 20-cv-577, 2020 WL 5530134 at *5 (N.D. Ill. Sept. 15, 2020) (determining that the fact that the defendant's "dataset" of "biometric measurements that ***can be used*** to identify plaintiff" was sufficient to "implicate BIPA" ***even if it was not actually used to identify them***.) (emphasis added); and *Carpenter v. McDonald's Corp.*, Case No.: 1:21-cv-02906, 2022 WL 897149 at *3 (N.D. Ill. Jan. 3, 2020) ("In the Court's view, pursuant to the plain language of the statute, a defendant may violate BIPA by collecting a voiceprint that ***merely could be used to identify a Claimant. The collection of a voiceprint-which is explicitly included in the definition of biometric identifier' without consent, even if not collected for the purpose of identifying that person, is a violation of the statute***.") (emphasis added).

Finally, Samsung is still in violation of BIPA even if it is true that the surreptitiously collected biometric data remains on the user's device and not on Samsung's servers. Illinois courts have rejected this argument. For instance, in *Hazlitt*, the plaintiffs alleged that Apple both collected and possessed their biometric data using facial recognition software that defendant "owned, exclusively controlled, and barred users from accessing, removing, or disabling." *Hazlitt v. Apple Inc,* 500 F. Supp. 3d 738 (S.D. Ill. 2020). In reaching its conclusion, the court rejected Apple's argument that plaintiffs' allegations were insufficient to establish possession or collection because the biometric data was "stored [only] locally on users' device[s]." *Id.* Similarly, in *Hazlitt II*, the Southern District of Illinois found a direct violation of Section 15(a) regardless of whether the biometric information is stored on the individual's device or the company's server. *See Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643, 645 (S.D. Ill. 2021) ("*Hazlitt II*").

Samsung is in violation of BIPA because it generates, collects, and stores users' biometric data without first obtaining informed user consent and does not have a publicly available retention schedule and guidelines for permanently destroying users' biometric identifiers and information.

For the past four (4) months, we have engaged in good faith efforts to resolve our clients' claims, but these efforts have been met with flat denials and threats of sanctions. It is clear we are now at an impasse. As such, we are filing the first 50,000 tranche of claims today.

Sincerely yours,

Jonathan Gardner